UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/718,041	11/20/2000	Charles A. Kunzinger	RSW920000100US1	2219

7590 01/12/2005

Gerald R Woods
IBM Corporation
T81/503
P O Box 12195
Research Triangle Park, NC 27709

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/718,041	KUNZINGER, CHARLES A.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover she t with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31 and 33-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *36 and 37* is/are allowed.

6)☒ Claim(s) *1-3,5-14,16-22,24-30 and 33-35* is/are rejected.

7)☐ Claim(s) *4,15,23 and 31* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 and 33-37 have been examined. Applicant in the amendment filed on October 27, 2004 amended claims 1, 3, 4, 14, 15, 22, 23, 28, 30, 31 and 36, added new claim 37 and canceled claim 32.

Response to Amendment

2. The 112, second paragraph rejection to claim 32 is withdrawn as the claim has been canceled.

Response to Arguments

3. The following is a response to the arguments presented on pgs. 17-20 in the amendment filed on October 27, 2004.

4. Applicant's arguments, with respect to amended independent claim 36 have been fully considered and are persuasive. The rejection of claim 36 has been withdrawn.

5. Regarding Applicant's argument that the Stalling reference does not teach a first security association between a first host and a boundary device and a second security association between a second host and the boundary device (see Remarks, pg. 18, last paragraph), examiner disagrees. The Stallings reference on pg. 411, Figure 13.5 explicitly depicts a security association between a host and a boundary device; implicit

in the End-to-intermediate-authentication example are a plurality of hosts to authenticate with the boundary device.

6. Applicant's arguments with respect to claim 28 (see Remarks, pg. 19, last paragraph) have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 2, 5, 6-13, 16-21 and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings) in view of Boyle U.S. Patent No. 5,940,591 (hereinafter Boyle).

9. As per claims 1 and 5, Stallings discloses a computer network security apparatus for providing coarse-grained access control in a computer networking environment, the apparatus embodied on one or more computer-readable media and comprising:

a. computer-readable program code means for establishing a first security association between a first host and a boundary device, wherein the first security association uses strong cryptographic techniques (see Stallings, page 411,

Figure 13.5, 'End-to-intermediate authentication'; page 404-407, 'Security Associations', especially first paragraph in section);

b. computer-readable program code means for establishing a second security association between a second host and the boundary device, wherein the second security association uses strong cryptographic techniques (see Stallings, page 411, Figure 13.5, 'End-to-intermediate authentication'; page 404-407, 'Security Associations', especially first paragraph in section);

c. computer-readable program code means for extracting, by a security enforcement function in the boundary device, a first authenticated identity associated with the first host during operation of the computer-readable program code means for establishing the first security association (see Stallings, page 412, Figure 13.6 and first paragraph, 3rd full sentence);

d. computer-readable program code means for extracting, by the security enforcement function in the boundary device, a second authenticated identity association with the second host during operation of the computer-readable program means for establishing the second security association (see Stallings, page 412, Figure 13.6 and first paragraph, 3rd full sentence);

e. computer-readable program code means for providing the extracted first authenticated identity and the extracted second authenticated identity, by the security enforcement function to an access control function (see Stallings, page 412, Figure 13.6 and first paragraph, 3rd full sentence); and

f. computer-readable program code means for determining access privileges of the first host and the second host, by the access control function, based upon the provided extracted identities (see Stallings, page 404, Table 13.1, 'Access Control'; page 412, first paragraph, 3rd full sentence).

10. Stallings does not expressly disclose the security enforcement function and the access control function as being in separate devices and hence requiring a secure channel between the two functions. Boyle teaches a network security configuration wherein a secure channel is established between a security enforcement function contained in a boundary device and an access control function contained in a security manager. See Boyle, Figure 2; col. 7, lines 55-58; col. 8, lines 39-51, especially lines 45-47 and 50; claim 2; Note, Figure 2 illustrates several examples wherein the SNIU are implemented for internetwork connections (i.e. networking layer). It would be obvious to one of ordinary skill in the art at the time the invention was made for the security enforcement function to be situated in a boundary device and the access control function to be situated in a security manager wherein communications between the two functions are secured as taught by Boyle since this configuration enables administrative policies to be centralized in a single unit, modularizes the devices of the architecture by dividing labor into their respective devices, and secures distribution of administrative directives in a secure channel. See Boyle, Figure 2; col. 2, lines 59-62.

11. Finally, the network security configuration disclosed by Boyle implements a fine-grained, identity-based access control methodology administered by the security manager, wherein the authenticated identities are used to determine access privileges

of the hosts. See Boyle, col. 5, lines 29-60; Figure 6A; claim 2. It would be obvious to one of ordinary skill in the art at the time the invention was made for the access controls to be based on the identities of the communicating entities since doing so restricts access based on user-defined attributes. See Boyle, col. 1, lines 44-46. The aforementioned cover the limitations of claims 1 and 5.

12. As per claim 2, Stallings covers an apparatus as outlined above in the claim 1 rejection. In addition, the strong cryptographic techniques used for the first security association and second security association are provided by protocols known as IKE and IPsec. See pages 402-408, section 13.2, 'IP Security Architecture' and pages 421-431, section 13.6, 'Key Management'. The aforementioned cover the limitations of claim 2.

13. As per claims 6 and 9, Stallings covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the security associations defined by Stallings specify only coarse-grained access control information. See Stallings, pages 402-408, section 13.2 'IP Security Architecture'; see applicant's specification page 7, 2nd paragraph, 2nd sentence for basis of "coarse-grained" access control use in IPsec. The aforementioned cover the limitations of claims 6 and 9.

14. As per claims 7, 8, 10 and 11, Stallings covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the authenticated identities

associated with the hosts are an identification of a user or an application on the hosts. See Stallings, page 401, Figure 13.1. The aforementioned cover the limitations of claims 7, 8, 10 and 11.

15. As per claims 12, 13, 16, 18 and 19, they are system claims corresponding to claims 1, 2 and 6-11, and they do not teach or define above the information claimed in claims 1, 2 and 6-11. Therefore, claims 12, 13, 16, 18 and 19 are rejected as being unpatentable over Stallings in view of Boyle for the same reasons set forth in the rejections of claims 1, 2 and 6-11.

16. As per claim 17, Stallings covers a system as outlined above in the claim 5 and 12 rejections under 35 U.S.C. 103(a). In addition, the security enforcement functions are located in the first and second hosts. See Stallings, page 401, Figure 13.1, 'User system with IPSec'. The aforementioned cover the limitations of claim 17.

17. As per claims 20, 21 and 24-27, they are method claims corresponding to claims 12, 13 and 16-19 and they do not teach or define above the information claimed in claims 12, 13 and 16-19. Therefore, claims 20, 21 and 24-27 are rejected as being unpatentable over Stallings in view of Boyle for the same reasons set forth in the rejections of claims 12, 13 and 16-19.

18. Claims 3, 14, 22, 28-30 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Boyle, and further in view of Jason et al. U.S. Patent No. 6,636,520 (hereinafter Jason).

19. As per claim 3, Stallings covers an apparatus as outlined above in the claim 1 rejection. In addition, the apparatus further comprises:

a. computer-readable program code means for securely making the determined access privileges available to the security enforcement function and using the access privileges to forward packets between hosts or discard the packet (see Boyle, col. 8, lines 45-47).

20. Stallings does not expressly teach forwarding a packet between the first host and the second host using the first and second security associations. Jason teaches a means for forwarding a packet between a first host and a second host using a first and second security association as IPsec tunnels. See Jason, Figure 2; col. 4:28-65. It would be obvious to one of ordinary skill in the art at the time the invention was made to forward a packet between the first host and the second host using the first and second security associations once access privileges were ascertained and approved. Motivation to combine enables a path between two nodes to incorporate a plurality of security associations. See Jason, Ibid. The aforementioned cover the limitations of claim 3.

21. As per claim 14, it is a system claim corresponding to claims 3 and 12, and it does not teach or define above the information claimed in claims 3 and 12. Therefore, claim 14 is rejected as being unpatentable over Stallings in view of Boyle and Jason for the same reasons set forth in the rejections of claims 3 and 12.

22. As per claim 22, it is a method claim corresponding to claims 3 and 20, and it does not teach or define above the information claimed in claims 3 and 20. Therefore, claim 22 is rejected as being unpatentable over Stallings in view of Boyle and Jason for the same reasons set forth in the rejections of claims 3 and 20.

23. As per claim 28, Stallings covers a method as outlined above in the claim 3 rejection under 35 U.S.C. 103(a). In addition, the method includes a first security association between a first host and a first boundary device, a second security association between a second host and a second boundary device, and a third security association between the first boundary device and the second boundary device (see Stallings, pg. 411, Figure 13.5, 'End-to-Intermediate Authentication'; see Jason, Figure 3). The aforementioned cover the limitations of claim 28.

24. As per claims 29, 30 and 33-35, they are method claims corresponding to claims 20, 21 and 24-28, and they do not teach or define above the information claimed in claims 20, 21 and 24-28. Therefore, claims 29, 30 and 33-35 are rejected as being

unpatentable over Stallings in view of Boyle and Jason for the same reasons set forth in the rejections of claims 20, 21 and 24-28.

Allowable Subject Matter

25. Claims 4, 15, 23 and 31 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

26. Claims 36 and 37 are allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
January 6, 2005

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100